

On Symmetric SL-Invariant Polynomials in Four Qubits

Gilad Gour^{1,*} and Nolan R. Wallach^{2,†}

¹*Institute for Quantum Information Science and Department of Mathematics and Statistics,
University of Calgary, 2500 University Drive NW, Calgary, Alberta, Canada T2N 1N4*

²*Department of Mathematics, University of California/San Diego, La Jolla, California 92093-0112*

We find the generating set of SL-invariant polynomials in four qubits that are also invariant under permutations of the qubits. The set consists of four polynomials of degrees 2,6,8, and 12, for which we find an elegant expression in the space of critical states. In addition, we show that the Hyperdeterminant in four qubits is the only SL-invariant polynomial (up to powers of itself) that is non-vanishing precisely on the set of generic states.

I. INTRODUCTION

With the emergence of quantum information science in recent years, much effort has been given to the study of entanglement [1]; in particular, to its characterization, manipulation and quantification [2]. It was realized that highly entangled states are the most desirable resources for many quantum information processing tasks. While two-party entanglement was very well studied, entanglement in multi-qubit systems is far less understood. Perhaps one of the reasons is that n qubits (with $n > 3$) can be entangled in an uncountable number of ways [3–5] with respect to stochastic local operations assisted by classical communication (SLOCC). It is therefore not very clear what role entanglement measures can play in multi-qubits or multi-qudits systems unless they are defined operationally. One exception from this conclusion are entanglement measures that are defined in terms of the absolute value of SL-invariant polynomials [4–11].

Two important examples are the concurrence [12] and the square root of the 3-tangle (SRT) [11]. The concurrence and the SRT, respectively, are the only $SL(2, \mathbb{C}) \otimes SL(2, \mathbb{C})$ and $SL(2, \mathbb{C}) \otimes SL(2, \mathbb{C}) \otimes SL(2, \mathbb{C})$ invariant measures of entanglement that are homogenous of degree 1. The reason is that in two and three qubit systems there is a unique homogeneous SL-invariant polynomial (up to scalar multiple) such that all other homogeneous invariant polynomials are multiples of powers of it. However for 4 qubits or more, the picture is different since there are many algebraically independent homogenous SL invariant polynomials such as the 4-tangle [6] or the Hyperdeterminant [10].

In this note, we find the generating set of all SL-invariant polynomials with the property that they are also invariant under any permutation of the four qubits. Such polynomials yield measure of entanglement that capture genuine 4 qubits entanglement. In addition, we show that the 4-qubit Hyperdeterminant [10] is the only homogeneous SL-invariant polynomial (of degree 24) that is non-vanishing precisely on generic states.

This note is written with a variety of audiences in mind. First and foremost are the researchers who study quantum entanglement. We have therefore endeavored to keep the mathematical prerequisites to a minimum and have opted for proofs that emphasize explicit formulas for the indicated SL -invariant polynomials. We are aware that there are shorter proofs of the main results using the important work of Vinberg. However, to us, the most important aspect of the paper is that the Weyl group of F_4 is built into the study of entanglement for 4 qubits. Indeed, the well known result of Shepherd-Todd on the invariants for the Weyl group of F_4 gives an almost immediate proof of Theorem 1. The referee has indicated a short proof of Theorem 5 using more algebraic geometry. Although our proof is longer, we have opted to keep it since it is more elementary. We should also point out that in the jargon of Lie theory the hyperdeterminant is just the discriminant for the symmetric space corresponding to $SO(4;4)$.

II. SYMMETRIC INVARIANTS

Let $H_n = \otimes^n \mathbb{C}^2$ denote the space of n -qubits, and let $G = SL(2, \mathbb{C})^{\otimes n}$ act on H_n by the tensor product action. An SL -invariant polynomial, $f(\psi)$, is a polynomial in the components of the vector $\psi \in H_n$, which is invariant under the action of the group G . That is, $f(g\psi) = f(\psi)$ for all $g \in G$. In the case of two qubits the SL invariant polynomials

*Electronic address: gour@ucalgary.ca

†Electronic address: nwallach@ucsd.edu

are polynomials in the f_2 given by the bilinear form (ψ, ψ) :

$$f_2(\psi) \equiv (\psi, \psi) \equiv \langle \psi^* | \sigma_y \otimes \sigma_y | \psi \rangle, \quad \psi \in \mathbb{C}^2 \otimes \mathbb{C}^2,$$

where σ_y is the second 2×2 Pauli matrix with i and $-i$ on the off-diagonal terms. Its absolute value is the celebrated concurrence [12].

In the case of three qubits all SL invariant polynomials are polynomials in the f_4 described as follows:

$$f_4(\psi) = \det \begin{bmatrix} (\varphi_0, \varphi_0) & (\varphi_0, \varphi_1) \\ (\varphi_1, \varphi_0) & (\varphi_1, \varphi_1) \end{bmatrix},$$

where the two qubits states φ_i for $i = 0, 1$ are defined by the decomposition $|\psi\rangle = |0\rangle|\varphi_0\rangle + |1\rangle|\varphi_1\rangle$, and the bilinear form (φ_i, φ_j) is defined above for two qubits. The absolute value of f_4 is the celebrated 3-tangle [13].

In four qubits, however, there are many independent SL -invariant polynomials and it is possible to show that they are generated by four SL-invariant polynomials (see e.g. [4] for more details and references). Here we are interested in SL-invariant polynomials that are also invariant under the permutation of the qubits.

Consider the permutation group S_n acting by the interchange of the qubits. Let \tilde{G} be the group $S_n \ltimes G$. That is, the set $S_n \times G$ with multiplication

$$(s, g_1 \otimes g_2 \otimes \cdots \otimes g_n)(t, h_1 \otimes h_2 \otimes \cdots \otimes h_n) = (st, g_{t1}h_1 \otimes g_{t2}h_2 \otimes \cdots \otimes g_{tn}h_n).$$

Then \tilde{G} acts on H_n by these two actions. We are interested in the polynomial invariants of this group action.

One can easily check that f_2 and f_4 above are also \tilde{G} -invariant. However, this automatic \tilde{G} -invariance of G -invariants breaks down for $n = 4$. As is well known [4], the polynomials on H_4 that are invariant under G are generated by four polynomials of respective degrees 2, 4, 4, 6. For \tilde{G} we have the following theorem:

Theorem 1 *The \tilde{G} -invariant polynomials on H_4 are generated by four algebraically independent homogeneous polynomials h_1, h_2, h_3 and h_4 of respective degrees 2, 6, 8 and 12. Furthermore, the polynomials can be taken to be $\mathcal{F}_1(z), \mathcal{F}_3(z), \mathcal{F}_4(z), \mathcal{F}_6(z)$ as given explicitly in Eq. (1) of the proof.*

Proof. To prove this result we will use some results from [4]. Let

$$u_0 = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle),$$

$$u_1 = \frac{1}{2}(|0000\rangle - |0011\rangle - |1100\rangle + |1111\rangle),$$

$$u_2 = \frac{1}{2}(|0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle),$$

$$u_3 = \frac{1}{2}(|0101\rangle - |0110\rangle - |1001\rangle + |1010\rangle).$$

Let A be the vector subspace of H_4 generated by the u_j . Then GA contains an open subset of H_4 and is dense. This implies that any G -invariant polynomial on H_4 is determined by its restriction to A . Writing a general state in A as $z = \sum z_i u_i$, we can choose the invariant polynomials such that their restrictions to A are given by

$$\mathcal{E}_0(z) = z_0 z_1 z_2 z_3, \quad \mathcal{E}_j(z) = z_0^{2j} + z_1^{2j} + z_2^{2j} + z_3^{2j}, \quad j = 1, 2, 3.$$

In [4] we give explicit formulas for their extensions to H_4 .

Also, let W be the group of transformations of A given by $\{g \in G | gA = A\}_{|A}$. Then W is the finite group of linear transformations of the form

$$u_i \longmapsto \varepsilon_i u_{s^{-1}i}$$

with $\varepsilon_i = \pm 1$, $s \in S_4$ and $\varepsilon_0 \varepsilon_1 \varepsilon_2 \varepsilon_3 = 1$. One can show [4, 9] that every W -invariant polynomial can be written as a polynomial in $\mathcal{E}_0, \mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$. We now look at the restriction of the S_4 that permutes the qubits to A . Set $\sigma_i = (i, i+1)$,

$i = 1, 2, 3$ where, say, $(2, 3)$ corresponds to fixing the first and last qubit and interchanging the second and third. Then they have matrices relative to the basis u_j :

$$\sigma_{1|A} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix},$$

$$\sigma_{2|A} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix},$$

$$\sigma_{3|A} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

Since S_4 is generated by $(1, 2), (2, 3), (3, 4)$, it is enough to find those W -invariants that are also $\sigma_{i|A}$ invariant for $i = 1, 2$. We note that the only one of the \mathcal{E}_j that is not invariant under $\sigma_{1|A}$ is \mathcal{E}_0 and $\mathcal{E}_0(\sigma_1 z) = -\mathcal{E}_0(z)$ for $z \in A$. Thus if $F(x_0, x_1, x_2, x_3)$ is a polynomial in the indeterminates x_j then $F(\mathcal{E}_0, \mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3)$ is invariant under $\nu = \sigma_{1|A}$ if and only if x_0 appears to even powers. It is an easy exercise to show that if $\mathcal{E}_4 = z_0^8 + z_1^8 + z_2^8 + z_3^8$ then any polynomial in $\mathcal{E}_0^2, \mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ is a polynomial in $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3, \mathcal{E}_4$ and conversely (see the argument in the very beginning of the next section). Thus we need only find the polynomials in $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3, \mathcal{E}_4$ that are invariant under $\tau = \sigma_{2|A}$. A direct calculation shows that \mathcal{E}_1 is invariant under τ . Also,

$$\mathcal{E}_1^2 \circ \tau = \mathcal{E}_1^2, \quad \mathcal{E}_2 \circ \tau = \frac{3}{4}\mathcal{E}_1^2 - \frac{1}{2}\mathcal{E}_2 + 6\mathcal{E}_0, \quad \mathcal{E}_0 \circ \tau = -\frac{1}{16}\mathcal{E}_1^2 + \frac{1}{8}\mathcal{E}_2 + \frac{1}{2}\mathcal{E}_0.$$

Since $\mathcal{E}_0, \mathcal{E}_1^2, \mathcal{E}_2$ forms a basis of the W invariant polynomials of degree 4 this calculation shows that the space of polynomials of degree 4 invariant under τ, ν and W (hence under \widetilde{W}) consists of the multiples of \mathcal{E}_1^2 . The space of polynomials invariant under W and ν and homogeneous of degree 6 is spanned by $\mathcal{E}_1^3, \mathcal{E}_1\mathcal{E}_2$, and \mathcal{E}_3 . From this it is clear that the space of homogeneous degree 6 polynomials that are invariant under \widetilde{W} is two dimensional. Since \mathcal{E}_1^3 is clearly \widetilde{W} -invariant there is one new invariant of degree 6. Continuing in this way we find that to degree 12 there are invariants h_1, h_2, h_3, h_4 of degrees 2, 6, 8 and 12, respectively, such that: (1) the invariant of degree 8, h_3 , is not of the form $ah_1^4 + bh_1h_2$, (2) there is no new invariant of degree 10, and (3) the invariant of degree 12, h_4 , cannot be written in the form $ah_1^6 + bh_1^3h_2 + ch_1^2h_3$. To describe these invariants we write out a new set of invariants. We put

$$\mathcal{F}_k(z) = \frac{1}{6} \sum_{i < j} (z_i - z_j)^{2k} + \frac{1}{6} \sum_{i < j} (z_i + z_j)^{2k}. \quad (1)$$

We note that $\mathcal{F}_1 = \mathcal{E}_1, \mathcal{F}_2 = \mathcal{E}_1^2$. A direct check shows that these polynomials are invariant under \widetilde{W} . Since $\mathcal{F}_3(z) \neq c\mathcal{E}_1^3$ we can use it as the “missing polynomial”. If one calculates the Jacobian determinant of $\mathcal{F}_1(z), \mathcal{F}_3(z), \mathcal{F}_4(z), \mathcal{F}_6(z)$ then it is not 0. This implies that none of these polynomials can be expressed as a polynomial in the others. Thus they can be taken to be h_1, h_2, h_3, h_4 .

Let $A_{\mathbb{R}}$ denote the vector space over \mathbb{R} spanned by the u_j . If $\lambda \in A_{\mathbb{R}}$ is non-zero then we set for $a \in A$, $s_{\lambda}a = a - \frac{2\langle \lambda | a \rangle}{\langle \lambda | \lambda \rangle} \lambda$. Then such a transformation is called a reflection. It is the reflection about the hyperplane perpendicular to λ . The obvious calculation shows that $\nu = s_{u_3}$ and if $\alpha = \frac{1}{2}(u_0 - u_1 - u_2 - u_3)$ then $\tau = s_{\alpha}$. We note that \widetilde{W} is generated by the reflections corresponding to $u_0 - u_1, u_1 - u_2, u_2 - u_3$ and $u_2 + u_3$. This implies that the group \widetilde{W} is generated by reflections. One also checks that it is finite (actually of order 576). The general theory (cf. [14]) implies that the algebra of invariants is generated by algebraically independent homogeneous polynomials. Using this it is easy to see that $\mathcal{F}_1(z), \mathcal{F}_3(z), \mathcal{F}_4(z), \mathcal{F}_6(z)$ generate the algebra of invariants. ■

Remark 2 *Alternatively, we note that \widetilde{W} is isomorphic with the Weyl group of the exceptional group F_4 (see Bourbaki, Chapitres 4, 5, et 6 Planche VIII pp. 272, 273). The exponents (exposants on p. 273) are 1, 5, 7, 11. This implies that the algebra of invariants is generated by algebraically independent homogeneous polynomials of degrees one more than the exponents so 2, 6, 8, 12. We also note that the basic invariants for F_4 were given as $\mathcal{F}_1(z), \mathcal{F}_3(z), \mathcal{F}_4(z), \mathcal{F}_6(z)$ for the first time by M.L.Mehta, Comm. Algebra, 16(1988), pp. 1083-1098.*

For $n \geq 4$ qubits the analogue of the space A would have to be of dimension $2^n - 3n$. Thus even if there were a good candidate one would be studying, say, for 5 qubits, a space of dimension 17 and an immense finite group that cannot be generated by reflections.

III. A SPECIAL INVARIANT (HYPERDETERMINAT) FOR 4 QUBITS.

In this section we show that the hyperdeterminant for qubits is the only polynomial that quantifies genuine 4-way generic entanglement. We start by observing that Newton's formulas (relating power sums to elementary symmetric functions) imply that if a_1, \dots, a_n are elements of an algebra over \mathbb{Q} (the rational numbers) then

$$a_1 a_2 \cdots a_n = f_n(p_1(a_1, \dots, a_n), \dots, p_n(a_1, \dots, a_n))$$

with f_n a polynomial with rational coefficients in n indeterminates and $p_i(x_1, \dots, x_n) = \sum x_j^i$. This says that in the notation of the previous theorem

$$\gamma(z) = \prod_{i < j} (z_i - z_j)^2 (z_i + z_j)^2$$

is \widetilde{W} -invariant. Indeed, take $a_1, \dots, a_{n(n-1)}$ to be $\{(z_i - z_j)^2 | i < j\} \cup \{(z_i + z_j)^2 | i < j\}$ in some order. We will also use the notation γ for the corresponding polynomial of degree 24 on H_4 .

We define the generic set, Ω , in H_4 to be the set of elements, v , such that $\dim Gv$ is maximal (that is, 12). Then every such element can be conjugated to an element of A by an element of G . It is easily checked that

$$\Omega \cap A = \left\{ \sum z_i u_i \mid z_i \neq \pm z_j \text{ if } i \neq j \right\}.$$

This implies that $\Omega = \{\phi \in H_4 \mid \gamma(\phi) \neq 0\}$.

Proposition 3 *If f is a polynomial on H_4 that is invariant under the action of G and is such that $f(H_4 - \Omega) = 0$ then f is divisible by γ .*

Proof. Since $f(z) = 0$ if $z_i = \pm z_j$ for $i \neq j$ we see that f is divisible by $z_i - z_j$ and $z_i + z_j$ for $i < j$. Thus if

$$\Delta(z) = \prod_{i < j} (z_i - z_j)(z_i + z_j)$$

then $f = \Delta g$ with g a polynomial on A . One checks that $\Delta(sz) = \det(s)\Delta(z)$ for $s \in W$ (see the notation in the previous section). Since $f(sz) = f(z)$ for $s \in W$ we see that $g(sz) = \det(s)g(z)$ for $s \in W$. But this implies that $g(z) = 0$ if $z_i = \pm z_j$ for $i \neq j$. So g is also divisible by Δ . We conclude that f is divisible by Δ^2 . This is the content of the theorem. ■

Lemma 4 *γ is an irreducible polynomial.*

Proof. Let $\gamma = \gamma_1 \gamma_2 \cdots \gamma_m$ be a factorization into irreducible (non-constant) polynomials. If $g \in G$ then since the factorization is unique up to order and scalar multiple there is for each $g \in G$, a permutation $\sigma(g) \in S_m$ and $c_i(g) \in \mathbb{C} - \{0\}$, $i = 1, \dots, m$ such that $\gamma_j \circ g^{-1} = c_j(g) \gamma_{\sigma(g)j}$ for $j = 1, \dots, m$. The map $g \mapsto \sigma(g)$ is a group homomorphism. The kernel of σ is a closed subgroup of G . Thus $G/\ker \sigma$ is a finite group that is a continuous image of G . So it must be the group with one element since G is connected. This implies that each γ_j satisfies $\gamma_j \circ g^{-1} = c_j(g) \gamma_j$ for all $g \in G$. We therefore see that $c_j : G \rightarrow \mathbb{C} - \{0\}$ is a group homomorphism for each j . But the commutator group of G is G . Thus $c_j(g) = 1$ for all g . This implies that each of the factors γ_j is invariant under G . Now each $\gamma_{j|A}$ divides $\gamma_{|A}$ thus in must be a product

$$\prod_{i < j} (z_i - z_j)^{a_{ij}} (z_i + z_j)^{b_{ij}}$$

by unique factorization. We note that if $i < j$ then $\{(z_i + z_j) \circ s \mid s \in W\} = \{(z_i - z_j) \circ s \mid s \in W\} = \{\varepsilon(z_i + z_j) \mid i < j, \varepsilon \in \{\pm 1\}\} \cup \{z_i - z_j \mid i \neq j\}$. This implies that since $\gamma_{j|A}$ is non-constant and W -invariant that each $\gamma_{j|A}$ must be divisible by $\Delta_{|A}$. Now arguing as in the previous proposition the invariance implies that γ_j is divisible by $\Delta^2 = \gamma$. This implies that $m = 1$. ■

Theorem 5 *If f is a polynomial on H_4 such that $f(\phi) \neq 0$ for $\phi \in \Omega$ then there exists $c \in \mathbb{C}$, $c \neq 0$ and r such that $f = c\gamma^r$.*

Proof. We may assume that f is non-constant. Let h be an irreducible factor of f . Then $h(\phi) \neq 0$ if $\phi \in \Omega$. This implies that the irreducible variety $Y = \{x \in H_4 | h(x) = 0\} \subset H_4 - \Omega = \{x \in H_4 | \gamma(x) = 0\}$. Since the variety $H_4 - \Omega$ is irreducible, and since both varieties are of dimension 15 over \mathbb{C} they must be equal. This implies that h must be a multiple of γ . Since f factors into irreducible non-constant factors the theorem follows. ■

IV. DISCUSSION

In this note we have shown that the set of all 4-qubit SL-invariant polynomials that are also invariant under permutations of the qubits is generated by four polynomials of degrees 2,6,8,12. Using a completely different approach, in [8] it was also shown that these polynomials exist but they were not given elegantly as in Eq. (1). In addition, we have shown here that the Hyperdeterminant [10] is the *only* SL-invariant polynomial (up to its powers) that is not vanishing precisely on the set of generic states.

Since the Hyperdeterminant (in our notations $\gamma(z)$) quantifies generic entanglement, a state with the most amount of generic entanglement can be defined as a state, z , that maximize $|\gamma(z)|$. We are willing to conjecture that the state

$$|L\rangle = \frac{1}{\sqrt{3}}(u_0 + \omega u_1 + \bar{\omega} u_2) \ , \ \omega \equiv e^{i\pi/3} \ ,$$

is the unique state (up to a local unitary transformation) that maximizes $|\gamma(z)|$. Our conjecture is based on numerical tests. In addition, one can prove that $|L\rangle$ is a critical point for $|L\rangle$ in the sphere and the Hessian on the sphere is negative semi-definite.

It was shown in [4] that the state $|L\rangle$ maximizes uniquely many measures of 4 qubits entanglement. Moreover, one can easily check that the state $|L\rangle$ is the only state for which $\mathcal{E}_0 = \mathcal{E}_1 = \mathcal{E}_2 = 0$ while $\mathcal{E}_3(|L\rangle) = 1/9$. It is known that a state with such a property is unique and called cyclic [15, 16]. Similarly, we found out the unique state, $|F\rangle$ for which $\mathcal{F}_1(|F\rangle) = \mathcal{F}_3(|F\rangle) = \mathcal{F}_4(|F\rangle) = 0$ but $\mathcal{F}_6(|F\rangle) \neq 0$. The (non-normalized) unique state (up to a local unitary transformation) is

$$|F\rangle = (3 - \sqrt{3})u_0 + (1 + i)\sqrt{3}u_1 + (1 - i)\sqrt{3}u_2 - i(3 - \sqrt{3})u_3 \ .$$

Acknowledgments:— GG research is supported by NSERC.

-
- [1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
 - [2] M. B. Plenio and S. Virmani, Quant. Inf. Comp. **7**, 1 (2007).
 - [3] W. Dr, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
 - [4] G. Gour and N. Wallach, J. Math. Phys. **51** (11), 112201 (2010).
 - [5] F. Verstraete *et al*, Phys. Rev. A **68**, 052112 (2003).
 - [6] A. Uhlmann, Phys. Rev. A **62**, 032307 (2000); S. S. Bullock *et al*, J. Math. Phys. **45**, 2447 (2004).
 - [7] J.-G. Luque *et al*, Phys. Rev. A **67**, 042303 (2003).
 - [8] A. Osterloh *et al*, Phys. Rev. A **72**, 012337 (2005); D. Z. Dokovic *et al*, J. Math. Phys. **50**, 033509 (2009).
 - [9] N. R. Wallach, Notes from Venice C.I.M.E. June (2004). <http://www.math.ucsd.edu/~nwallach/venice.pdf>
 - [10] A. Miyake, Phys. Rev. A **67**, 012108 (2003); A. Miyake *et al*, Quant. Info. Comp. **2** (Special), 540 (2002).
 - [11] V. Coffman *et al*, Phys. Rev. A **61**, 052306 (2000)
 - [12] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
 - [13] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).
 - [14] J. E. Humphreys, "Reflection groups in Coxeter groups", Cambridge studies in advanced mathematics, Theorem 3.5 p. 54
 - [15] Bertram Kostant, "The Principal Three-Dimensional Subgroup and the Betti Numbers of a Complex Simple Group", American Journal of Mathematics, **81**(1959),973-1032.
 - [16] Bertram Kostant , "Lie Group Representations on Polynomial Rings", American Journal of Mathematics, **85** (1963), 327-404.